Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (canceled)

2. (previously presented) The method of claim 46, wherein the network security protocol is SSL (v3).

3. (previously presented) The method of claim 46, wherein the network security protocol is TLS.

4.-27. (canceled)

28. (previously presented) The method of claim 46 comprising aligning the received set of header data for the first packet.

29. (previously presented) The method of claim 28 comprising storing the aligned set of header data for the first packet in a FIFO to accumulate a predefined amount of data before commencing the authentication operations.

30. (previously presented) The method of claim 29 wherein the predefined amount of data comprises 512 bits.

31. (canceled).

32. (previously presented) The method of claim 28 where the aligned set of header data for the first packet comprises Content Type and Length that is aligned into rows of data where each row of data contains a single type of data.

33. (previously presented) The method of claim 46 comprising aligning, for encryption operations, the set of data in the payload data for the first packet to provide the aligned data for the encryption operations.

34. (previously presented) The method of claim 33 wherein aligning, for encryption operations, comprises removing non-valid data.

35. (previously presented) The method of claim 33 wherein aligning, for encryption operations, comprises adding padding.

36. (previously presented) The method of claim 33 comprising storing the aligned set of data in the payload data for the first packet for the encryption operations in a FIFO to accumulate a predefined amount of data before commencing the encryption operations.

37.-43. (canceled)

44. (previously presented) The method of claim 46 wherein:

the authentication operations are performed by an authentication component of the chip;

the encryption operations are performed by an encryption component of the chip; and

authentication data generated by the authentication component is passed to the encryption component and aligned by the encryption component.

45. (previously presented) The method of claim 46 wherein:

the authentication operations are performed by an authentication component of the chip;

the encryption operations are performed by an encryption component of the chip; and

decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component.

46. (currently amended) A method for accelerating cryptographic processing of a plurality of data packets according to a network security protocol, comprising:

receiving, in a chip, header data and payload for a first packet from an off-chip processor;

performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code;

performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet is performed in parallel with the authentication operations for the first packet;

receiving, in the chip, header data and payload data for a second packet;

<u>combining remaining payload data for the first packet with the authentication code for the first packet;</u>

adding padding to the combined remaining payload data ~~for the first packet~~ and ~~the~~ authentication code for the first packet to generate a first packet data block having a predefined length;

performing encryption operations on ~~the remaining payload data for~~ the first packet data block~~, the authentication code for the first packet, and the padding~~;

performing authentication operations on a set of header data and the payload data for the second packet, wherein the authentication operations on the set of header data and payload data for the second packet is performed simultaneously with the encryption operations on ~~the remaining payload data and authentication code for~~ the first packet data block; and

passing the cryptographically processed first packet from the chip to the off-chip processor,

wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass.